N69-18994
NASA CR-100185

FINAL REPORT FOR FIRST YEAR

(Sept. 16, 1967 to Sept. 15, 1968)

NASA GRANT NGL 15-004-026

"CONVOLUTIONAL CODING TECHNIQUES FOR DATA PROTECTION"

CASE FILE COPY

Department of

ELECTRICAL ENGINEERING

UNIVERSITY OF NOTRE DAME, NOTRE DAME, INDIANA

February 3, 1969

FINAL REPORT FOR FIRST YEAR

(Sept. 16, 1967 to Sept. 15, 1968)

NASA GRANT NGL 15-004-026

CASE COP

"CONVOLUTIONAL CODING TECHNIQUES FOR DATA PROTECTION"

Submitted to:
National Aeronautics & Space Administration
Office of Scientific & Technical Information (Code US)
Washington, D. C. 20546

Info. copy to:
Flight Data Systems Branch
NASA Goddard Space Flight Center
Greenbelt, Md. 20771
ATT: Dr. Robert W. Rochelle (Code 710)

Submitted by:
Dr. James L. Massey (Principal Investigator)
Professor of Electrical Engineering
University of Notre Dame
Notre Dame, Ind. 46556

ABSTRACT

The principal results obtained under NASA Grant NGR-15-004-026 during the period Sept. 16, 1967 to Sept. 15, 1968 were the following:

(1) Easily programmable algorithms for the synthesis of good, long convolutional codes,

(2) A unified analysis of decoders for convolutional codes based on the use of stochastic sequential machines models,

(3) Demonstration of the existence of "good" classes of convolutional codes with "bad" error propagation properties,

(4) Development of necessary and sufficient conditions for linear sequential machines (i.e. convolutional encoders) to have feedforward inverses,

(5) Development of a simple conceptual approach to obtain the properties of the Fano sequential decoding algorithm,

(6) New bounds on minimum distance for convolutional codes,

(7) Development of a complete and unified theory for inverses of linear, time-invariant dynamical systems,

and (8) Further development and simplification between decoding procedures for the Bose-Chaudhuri-Hocquenghem codes and the synthesis of minimal length linear feedback shift-registers.

In addition to describing the above research, this report includes a listing of all personnel involved in the research performed under this grant.

I. Summary of Main Research Results

(1) Synthesis of Good, Long Convolutional Codes

In recognition of the fact that future space communications systems may well require the use of convolutional codes with constraint lengths well beyond those for which good codes were formerly known, an effort was made to develop algorithms for obtaining good, long codes with a modest amount of computer search time. These efforts met with considerable success yielding algorithms which have been programmed, for instance, to obtain good rate 1/2 binary codes out to a constraint length of 144 bits (72 information bits), well beyond twice the constraint length of codes obtained by earlier investigators. Details of this work may be found in:

D. J. Costello, Jr., "A Construction Technique for Random-Error Correcting Convolutional Codes," Tech. Rpt. No. EE-685, U. of Notre Dame, Notre Dame, Ind., May 1, 1968. (This paper has been accepted for publication in IEEE Transactions on Information Theory.)

(2) A Unified Analysis of Decoders for Convolutional Codes

It was evident to students of convolutional coding, that the conceptual foundations of this subject were in a primitive stage compared to that for the earlier, but less efficient, block coding. Various decoding procedures, viz. sequential decoding, feedback threshold decoding, definite decoding, semi-definite decoding, Viterbi semi-sequential decoding, etc., had been advanced for convolutional codes with very little understanding of the relationships between these various forms of decoders.

To reduce the conceptual confusion, an effort was made to find a common framework that could accommodate all these varied forms of decoders. The stochastic sequential machine model was ultimately settled upon and proved to be exceptionally simple and flexible for the task of describing decoders for convolutional codes. Through the use of this model, the first precise definition and exact calculation of the steady-state error probability for a feedback decoder was obtained. Conditions were also obtained which guarantee the superiority of feedback decoding to definite decoding in most practical situations. It was further shown that for the Viterbi algorithm (which is a maximum likelihood

decoding procedure for finite sequences) that the decoding error probability always tends to a definite limit for decoding of infinite sequences, and that under certain conditions this steady-state error probability is an exponentially decreasing function of the code constraint length. Further details may be found in:

T. N. Morrissey, Jr., "Analysis of Decoders for Convolutional Codes by Stochastic Sequential Machine Methods," Tech. Rpt. No. EE-682, Dept. of Elec. Engr., U. of Notre Dame, Notre Dame, Ind., May 1, 1968.

T. N. Morrissey, Jr., "A Unified Markovian Analysis of Decoders for Convolutional Codes," Tech. Rpt. No. EE-687, Dept. of Elec. Engr., U. of Notre Dame, Notre Dame, Ind., Oct. 24, 1968. (This paper has been accepted for publication in the IEEE Transactions on Information Theory.)

(3) "Good" Codes with "Bad" Error Propagation Properties

The possibility of catastrophic decoding error-propagation, i.e. of the possibility that a finite number of channel errors could trigger infinitely many decoding errors, has been a haunting consideration for users of convolutional codes with feedback decoders. It was sometimes thought that such a catastrophe might occur only with a poor code or with a poor decoding algorithm for a good code. These considerations led to a research effort that culminated in the demonstration of infinite classes of good codes ("good" in the sense that their feedback-decoding minimum distance is at least half that guaranteed obtainable by the Gilbert bound) that necessarily exhibit catastrophic error propagation when decoded by any reasonable feedback decoder. It was further shown that the defect in these codes which gives rise to the catastrophic failure is their small definite-decoding minimum distance. Details may be found in:

J. L. Massey, "Catastrophic Error-Propagation in Convolutional Codes," Proceedings of 11th Midwest Circuit Theory Symposium, U. of Notre Dame, Notre Dame, Ind., May 13-14, 1968, pp. 583-587.

(4) Feedforward Inverses of Linear Sequential Circuits

It had earlier been pointed out by the principal investigator that a second kind of catastrophic behavior is possible with convolutional codes, viz. the occurrence of infinitely many errors in the decoded information digits when only a finite number of errors had been made in decoding the channel sequences, and that this catastrophe was avoidable if and

only if the linear sequential machine which serves as the convolutional encoder possesses a feedforward (i.e. feedback-free) inverse. This fact led to a successful effort to obtain the general conditions for the existence of a feedforward inverse of a linear sequential circuit. Details may be found in:

R. R. Olson, "Note on Feedforward Inverses of Linear Sequential Circuits," Tech. Rpt. No. EE-684, Dept. of Elec. Engr., U. of Notre Dame, April 1, 1968. (This paper has been submitted to the IEEE Transactions on Computers with the decision on publication still pending.)

(5) A Simple Conceptual Approach to the Fano Algorithm

The Fano algorithm has for several years been accepted as the best available sequential decoding algorithm, but understanding of the search properties of this algorithm has proved elusive. Research under this grant has led to an analysis of the Fano algorithm which makes derivation of the search properties both simple and intuitively pleasing. The basic steps in this procedure were first to consider the "searching" of a single path or trunk in which there are no alternate branches stemming from the nodes thereon, and second, to isolate a superposition principle by which the general tree-searching properties of the algorithm can readily be inferred from its trunk-searching properties. Details may be found in:

J. L. Massey and M. K. Sain, "Trunk and Tree Searching Properties of the Fano Sequential Decoding Algorithm," Elec. Engr. Memo. No. EE-6817, Univ. of Notre Dame, Notre Dame, Ind., Oct. 1, 1968. Also appearing in Proceedings of 6th Annual Allerton Conf. on Ckt. and System Th., Univ. of Illinois, Oct. 2-4, 1968, pp. 153-160.

This approach was also used as the foundation of an analysis of the statistical properties of the Fano algorithm that will be described in a forthcoming technical report. This result was described orally as:

J. L. Massey and M. K. Sain, "Distribution of the Minimum Cumulative Metric for Sequential Decoding," presented at IEEE International Symposium on Information Theory, Ellenville, N. Y., Jan. 28-31, 1969.

(6) Bounds on Minimum Distance of Convolutional Codes

One of the research goals of this grant is the obtaining of good bounds

for the minimum distance of convolutional codes that can be used for the evaluation of known codes. This research has led to a simple and improved Plotkin-type upper bound on the feedback-decoding minimum distance of convolutional codes, and to a Gilbert-type lower bound on the definite-decoding minimum distance. This latter bound is especially important since it proves the existence of good convolutional codes that are free of both catastrophic forms of failure described in sections (3) and (4) above. Moreover, the method of proof for this bound was based on the demonstration that almost all linear feedback shift-registers produce no non-zero output sequence with a sparse population of non-zero digits. Since each such shift-register is an encoder for a cyclic block code, and conversely, this analysis is expected to be useful in attacking the elusive question as to whether there exist arbitrarily long cyclic codes with good distance properties. Details may be found in:

J. L. Massey, "Some Algebraic and Distance Properties of Convolutional Codes," appearing in Error Correcting Codes (Editor: H. B. Mann), John Wiley and Sons, Inc., New York, 1968, pp. 89-109.

(7) Inverses of Dynamical Systems

An unexpected bonus of the work performed under this grant arose from the realization by the investigators that their work on feedforward inverses of linear sequential circuits could be easily generalized to a complete theory for inverses of time-invariant dynamical systems, both time-continuous and time-discrete. Such inverses, commonly known as "whitening filters" from their application in filtering and prediction theory, play important roles in many current investigations in statistical communication theory and optimal control theory. The generalization was carried out and resulted in criteria for the existence of inverses considerably simpler than those previously known, and also to a simple, general procedure for the construction of the inverse system from knowledge of the structural matrices of the original system. This research also isolated a fundamental new parameter, called the inherent integration of a system, which is the least integral of the input to the system that can be recovered as the output of a second

linear time-invariant dynamical system in cascade with the first system. Details of this research may be found in:

M. K. Sain and J. L. Massey, "Invertibility of Linear Time-Invariant Dynamical Systems," Elec. Engr. Memo. No. EE-687, U. of Notre Dame, Notre Dame, Ind., Aug. 8, 1968. (This paper has been accepted for publication in IEEE Transactions on Automatic Control.)

(8) Bose-Chaudhuri-Hocquenghem Codes and Linear Shift-Registers

During the period reported herein, the principal investigator achieved substantial simplification of his work relating the synthesis of minimal length linear feedback shift-registers for producing a given finite sequence of digits to the problem of decoding the Bose-Chaudhuri-Hocquenghem codes. This work demonstrates that the Berlekamp decoding algorithm, which is the most efficient known general algorithm for decoding these cyclic codes, is more generally just an algorithm to solve the shift-register synthesis problem cited above. Details may be found in:

J. L. Massey, "Shift Register Synthesis and BCH Decoding," Elec. Engr. Memo. No. EE-684, U. of Notre Dame, Notre Dame, Ind., June 18, 1968. (This paper has been accepted for publication in IEEE Transactions on Information Theory.)

(9) Other Activity

In addition to the theoretical research described above, during the period reported herein, the investigators completed the assembly langugage programming of a channel simulator and Fano sequential decoder for the UNIVAC 1107 computer in the University of Notre Dame Computing Center. These programs permit the simulation of either a binary symmetric channel or an additive Gaussian noise channel for use in conjunction with the sequential decoding of any convolutional code of rates $\frac{1}{2}$, $\frac{1}{3}$, or $\frac{1}{4}$ and constraint length of 72 information bits or less. The operation of these programs requires about 100 microseconds per computation as computations are defined with sequential decoding. Extensive simulations have since been carried out on this facility and the results will be reported in a future technical report.

II. Personnel Engaged in Research Under this Grant

Table I gives a complete accounting of all personnel engaged in research under this grant during the period covered by this report. Source of support is shown, if different from this grant, for graduate research students performing research under the direction of the principal investigator.

NAME	CATEGORY	DATES OF RESEARCH ACTIVITY	SOURCE OF SUPPORT, IF OTHER THAN THIS GRANT	REMARKS
(1) Dr. James L. Massey	Principal Investigator	9/16/67 to 9/15/68		
(2) Dr. Michael K. Sain	Assistant Investigator	6/16/67 to 8/15/68		
(3) Dr. K. Vairavan	Research Assistant	6/16/67 to 9/15/68		Received Ph.D., June 1968
(4) Mr. J. Chang	Research Assistant	6/16/67 to 9/15/68		
(5) Mr. D. Costello	Research Assistant	9/16/67 to 9/15/68	NSF Traineeship	Ph.D. expected, June 1969
(6) Dr. T. Morrissey	Research Assistant	9/16/67 to 9/15/68	NASA Traineeship	Received Ph.D., Aug. 1968
(7) Mr. R. Olson	Research Assistant	9/16/67 to 9/15/68		Ph.D. expected, June 1969
(8) Mr. J. Brennan	Undergraduate Programming Asst.	6/16/67 to 9/15/68		

TABLE I. Personnel Involved in Research Under This Grant